LAW OFFICES OF RONALD A. MARRON, APLC
RONALD A. MARRON (SBN 175650)
ron@consumersadvocates.com
SKYE RESENDES (SBN 278511)
skye@consumersadvocates.com
3636 4th Avenue, Suite 202
San Diego, California 92103
Telephone:(619) 696-9006
Facsimile: (619) 564-6665

Attorneys for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

DENNIS HOGAN, on behalf of himself, all others similarly situated and the general public, Plaintiff, v. JETRO HOLDINGS, LLC, a Delaware limited liability company; JETRO CASH & CARRY ENTERPRISES, LLC, a Delaware limited liability company; RESTAURANT DEPOT, LLC, a Delaware limited liability company; Defendants.	Case No.: **'13CV0462 L WVG** CLASS ACTION **COMPLAINT FOR:** **1. NEGLIGENCE;** **2. GROSS NEGLIGENCE;** **3. BREACH OF CONTRACT;** **4. BREACH OF IMPLIED CONTRACT** **5. VIOLATION OF CALIFORNIA'S SHINE THE LIGHT LAW (CAL. CIV. CODE § 1798.82)** **6. VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW (CAL. BUS. & PROF. CODE §§ 17200, *et seq.*)** DEMAND FOR JURY TRIAL

Dennis Hogan, on behalf of himself, all others similarly situated, and the general public ("Plaintiff"), alleges against Defendants Jetro Holdings, LLC, Jetro Cash & Carry Enterprises, LLC and Restaurant Depot, LLC (collectively, "Defendants") the following upon his own knowledge, or where there is no personal knowledge, upon information and belief and the investigation of his counsel:

PRELIMINARY STATEMENT

1. This is a consumer class action brought to obtain redress for losses and damages sustained by Plaintiff and the Class (as herein defined) as a result of Defendants' failure to maintain the security of private and confidential financial and personal information ("hereinafter Personally Identifiable Information" or "PII;" PII also includes information as defined by California Civil Code § 1798.81.5(d)) of Defendants' credit and debit card customers at Defendants' stores. Further, Defendants filed to timely notify Jetro Cash & Carry and Restaurant Depot customers of their security breach until at least two weeks after Defendants learned that unauthorized individuals stole credit card and debit card information from Defendants' card processing systems.

2. Plaintiff was a member and customer of Defendants' stores and in the course of making purchases at Defendants' stores, Plaintiff used and paid by debit and/or credit card. In making purchases, Plaintiff and the Class were required by Defendants to confide and make available to Defendant, its agents and employees, private and confidential debit and credit card information. This information was entrusted to Defendants solely for the purposes of effectuating payment for purchases and with the expectation and implied mutual understanding that Defendants would strictly maintain the confidentiality of the information and safeguard it from theft or misuse.

3. Beginning on or about September 21, 2011 through November 18, 2011, unauthorized individuals obtained access to Defendants' card processing systems and stole credit and debit card information. On information and belief, Defendants first learned of the breach on November 9, 2011, when some of Defendants' customers complained to Defendants of credit card fraud after they used their cards at Defendants' stores. Despite Defendants' knowledge of the breach, Defendants delayed in notifying their member customers until November 28, 2011.

4. Again, beginning on or about November 7, 2012 through December 4, 2012, unauthorized individuals obtained access to Defendants' card processing systems and stole credit and debit card information. On information and belief, Defendants first learned of the breach on December 4, 2012, when some of Defendants' customers complained to Defendants of credit card fraud after they used their cards at Defendants' stores. Despite Defendants' knowledge of the breach, Defendants delayed in notifying their member customers until December 19, 2012.

5. As a result of the breaches of security, Plaintiff and the Class' debit cards and credit cards were exposed to and subjected to unauthorized charges; their bank accounts were overdrawn and credit limits exceeded; they were deprived of the use of their cards and access to their funds; their preauthorized charge relationships were disrupted; they were required to expend time, energy and expense to address to resolve these financial disruptions and mitigate the consequences.

JURISDICTION AND VENUE

6. This Court has original jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A), as amended by the Class Action Fairness Act of 2005, because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of

$5,000,000.00 and is a class action where Plaintiff, a member of the class, is from a different state than Defendants. On information and belief, more than two-thirds of the members of the class are citizens of a state different from Defendants. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

7. Personal jurisdiction is derived from the fact that the Defendants conduct business within the State of California and within this judicial district.

8. Venue is proper within this district pursuant to 28 U.S.C. § 1391(b)(2) because many of the acts and transactions occurred in this district and because Defendants:

(i) are authorized to conduct business in this district and have intentionally availed itself of the laws and markets within this district;

(ii) do substantial business in this district;

(iii) sell their food, equipment and supplies to customers residing in this district; and,

(iv) are subject to personal jurisdiction in this district.

THE PARTIES

9. At all times relevant to this matter, Plaintiff Dennis Hogan was a resident of Imperial Beach, California.

10. On information and belief, at all times relevant to this matter, Defendant Jetro Holdings, LLC ("Jetro Holdings") is a Delaware limited liability company that maintains its principal place of business and corporate headquarters in College Point, New York.

11. On information and belief, at all times relevant to this matter, Defendant Jetro Cash & Carry Enterprises, LLC ("Jetro Cash & Carry") is a Delaware limited liability company that maintains its principal place of business

and corporate headquarters in College Point, New York. Jetro Cash & Carry also maintains at least four store locations in California, and is a division of Jetro Holdings.

12. On information and belief, at all times relevant to this matter, Defendant Restaurant Depot, LLC ("Restaurant Depot") is a Delaware limited liability company that maintains its principal place of business and corporate headquarters in College Point, New York. Restaurant Depot also maintains at Regional Administrative & Purchasing Offices in Anaheim, California, as well store locations throughout California. Restaurant Depot is a division of Jetro Holdings.

13. Members of the putative class reside in California and throughout the United States.

14. Defendants own and operate cash and carry warehouses throughout the United States, including California, that provide one-stop shopping for customers buying food, equipment and supplies.

15. Plaintiff is informed and believes and thereon alleges that at all times herein mentioned the Defendants and Defendants' employees were the agents, servants and employees of Defendants, acting within the purpose and scope of that agency and employment.

FACTS

16. Defendants regularly serve the needs of restaurants and other business owners by selling bulk supplies and equipment.

17. Customers purchasing restaurant supplies or equipment from Defendants are required to become members and have membership cards. Plaintiff and the Class are members and customers of Restaurant Depot. The membership relationship creased a special relationship between Defendants and Plaintiff and the Class.

18. Defendants have invited and continue to invite customers, including Plaintiff and the Class, to make use of their credit and debit cards to pay for purchases at Defendants' stores. Based on this invitation Plaintiff and the Class made use of their credit and debit cards to pay for their purchases at their stores, which also created a special relationship between Defendants and Plaintiff and the Class.

19. By using the membership cards and credit and debit cards to purchase goods, Plaintiff and the Class were paying for, among other things, Defendants' administrative costs of data management and security.

20. Plaintiff and the Class paid more for goods they purchased from Defendants than they otherwise would have, had they known of Defendants' inadequate protection of their PII.

21. Additionally, purchases for restaurants tend to be larger than purchases for typical individual consumers, and are often made by more than one representative of a restaurant, so use of a credit or debit card for purchase of Defendant's merchandise is necessary for Defendants' customers.

22. In the course of making such purchases, Plaintiff and the Class confided their private and confidential credit and debit card information to Defendants solely for the purpose of enabling Defendants to effectuate such payments. Such data was confided based on the express and implied representations by Defendants and on the expectation and implied mutual understanding that the data would be protected and safeguarded from access from unauthorized individuals.

23. Defendants keep and maintain a database of all of Jetro Cash & Carry and Restaurant Depot customers who tender payment to Defendants by credit card and/or debit card. Defendants did not encrypt or protect information provided by customers to Defendants. Defendants' lax security measures allowed third-parties

to access Defendants' credit and debit card processing systems at will and access any and all information desired.

Data Breach One

24. On or about November 28, 2011, Defendants publicly announced for the first time that between September 21, 2011 and November 18, 2011, Defendants' credit and debit card processing systems had been breached, leading to the theft of credit and debit card information as they were being processed. The unauthorized parties obtained the names of cardholders, credit or debit card numbers, card expiration dates, and verification codes that were on the magnetic stripes of credit and debit cards (hereinafter "Breach One"). *See* **Exhibit 1**.

25. Lack of adequate security in Defendants' card processing systems enabled unidentified persons to place foreign software, known as malware, on Defendants' card processing systems, which provided the unidentified persons with access to consumer debit card, credit card, and possibly other electronic information then in transit and temporarily stored on the system, and then diverted this information to the unidentified persons. *See* **Exhibit 1**.

26. Defendants did not monitor their card processing systems for the presence of foreign software in a manner that would enable them to detect this intrusion, so that the breach of security and diversion of customer information was able to continue unnoticed for two months.

27. On or before November 9, 2011, Defendants learned that customers had experienced credit card fraud after they used their cards at Defendants' stores.

28. The security breach was not contained until on or about November 18, 2011.

29. Although Defendants first became aware of the breaches of its credit processing systems as early as November 9, 2011, Defendants failed to disclose

publicly that customers' PII had been accessed and stolen until on or after November 28, 2011.

30. The unidentified persons who obtained such access and stole customers' PII misused this data by making unauthorized charges against the debit and credit card accounts of Plaintiff and the Class.

Data Breach Two

31. Again, on or about December 19, 2012, Defendants publicly announced for the first time that between November 7, 2012 and December 5, 2012, Defendants' credit and debit card processing systems had been breached, again leading to the theft or credit and debit card information (hereinafter "Breach Two").

32. After December 19, 2012, Plaintiff received a correspondence from Defendants informing Plaintiff:

> We very recently determined that unauthorized individuals stole credit card and debit card information from the card processing system we use in some of our stores. You are receiving this letter because we believe your credit or debit card information may have been stolen. We are sending this notice as soon as practically possible taking into consideration that legal enforcement authorities are involved. This letter explains actions we have taken in response to the theft and described some action you can take to protect yourself against fraud. **Our commitment to Payment card security: We believe our systems were compliant with payment card industry standards at the time of the apparent intrusion.** Our payment systems are monitored on a 24/7 basis by Trustwave, a Company that since 1995 has provided thousands of organizations with data security solutions and expertise. Indeed over the past year we have expended

> considerable resources and costs upgrading the credit card processing systems at each of our locations to ensure they met those security mandates.
>
> **Actions we have taken:** We learned on December 4th 2012 that some of our customers had experienced credit card fraud after they used their card at some of our stores. We hired Trustwave, a leading computer forensic firm, on December 6th to investigate. Trustwave investigators are still in the process of identifying all the details and are continuing their investigation but have so far determined the intrusions first started on November 7th 2012. Trustwave and our Information Technology staff are comfortable that the breach has been contained as of December 5th 2012…

Exhibit 2.

33. Again, lack of adequate security in Defendants' card processing systems enabled unidentified persons to access consumers' PII. *See* **Exhibit 2**.

34. Defendants failed to adequately safeguard and protect Plaintiff and the Class' PII, so that unidentified persons were able to obtain access to such data within Defendants' card processing systems and/or in the course of transmission of the data to financial institutions.

35. Defendants knew or should have known that their security measures were inadequate and that their computer systems and/or network were vulnerable to attack because their network and computer systems had previously been compromised during Data Breach One.

36. Defendants did not monitor their card processing systems in a manner that would enable them to detect this intrusion, so that the breach of security and diversion of customer information was able to continue unnoticed for approximately one month.

37. Further, Defendants did nothing to update their inadequate protocols or otherwise implement adequate safeguards both before and, particularly, after Data Breach I and before Data Breach Two.

38. Before Data Breach One and particularly before Data Breach Two, Defendants' decision not to install and maintain appropriate firewalls on its networks, including the Payment Card Industry Data Security Standard ("PCI DSS"), which requires anyone collecting payment card information to install and maintain a firewall, and is standard in the retail industry, of which Defendants' businesses are a part, was willful, intentional, or reckless. Defendants' conduct complained of herein was also willful, intentional, or reckless within the meaning of California Civil Code § 1798.84(d).

39. On or before December 4, 2012, Defendants learned that customers had experienced credit card fraud after they used their cards at Defendants' stores.

40. The security breach was not contained until on or about December 5, 2012.

41. Although Defendants first became aware of the breaches of its credit processing systems as early as December 4, 2012, Defendants failed to disclose publicly that customers' PII had been accessed and stolen until on or after December 19, 2012.

42. The unidentified persons who obtained such access stole Plaintiff's and the Class' PII.

43. The unidentified persons who obtained Plaintiff's and the Class' PII misused this data by making unauthorized charges against the debit and credit card accounts of Plaintiff and the Class, causing Plaintiff injury in fact in the form of lost monies from financial accounts accessed as a result of Defendants' conduct as complained of herein.

44. Defendants' card processing systems had multiple security shortfalls, including, but not limited to, lack of properly monitoring solutions; failure to encrypt internal network traffic flowing between stores and processer; point-of-sale systems that were open to attack; insecure wireless connections; failure to follow PCI DSS; failure to take reasonable steps to protect the security of Plaintiff's and the Class' PII, and/or remote access deficiencies.

45. During the Class Period (as herein defined) Plaintiff Hogan maintain an account with North Island Credit Union, which he accessed with debit and credit cards issued by the bank. Mr. Hogan shopped at Defendants' stores in San Diego, California and used his North Island debit and credit cards to make purchases there. On or about November 2011, Plaintiff learned that fraudulent charges had been made to his North Island Credit Union account using his debit card number. Plaintiff has yet to be reimbursed for these unauthorized charges. Again, on or about December 2012, Plaintiff learned that fraudulent charges had been made to his North Island Credit Union account using his debit card number. Plaintiff has yet to be reimbursed for these unauthorized charges totally $2,400.00 to $6,200.00. As a result of each breach, in addition to his account being overdrawn and/or missing funds, Plaintiff had to pay additional charges to cancel his bank cards, seek reissue of new bank cards with different numbers, obtain new checks, deal with disrupted preauthorized automatic charge relationships, pay overage charges and late fees, and was required to expend time, energy and expense to address and resolve these financial disruptions and mitigate the consequences.

46. As a direct and proximate result of Defendants' failure to maintain the security of its customers' PII, Plaintiff and the Class suffered a disruption of their financial affairs, endangerment of their financial assets and resources, and loss of personal property in the form of monetary damages. Plaintiff and the Class have

also had to expend time, effort and money to address, correct, repair, and/or mitigate the consequences of the disruption of their financial affairs and to mitigate and avert the harm threatened to their financial assets and resources, including their credit reputations. Plaintiff and the Class have incurred out-of-pocket loss and damage. Plaintiff and the Class also remain exposed to the risk of fraud if Defendants are not enjoined from using inferior and/or inadequate methods of data security and inadequate and/or inferior data breach notice.

47. Plaintiff never experienced identity theft before Data Breach One and took substantial precautions to safeguard his PII both before Data Breach One and before Data Breach Two. The same sensitive PII stolen through Defendants' conduct as complained of herein is the same sensitive PII that was used to steal Plaintiffs' identity and funds.

48. Plaintiff and the Class suffered damages in the amount equal to the fraudulent amount charged to their accounts for which they have not been reimbursed. Additional out-of-pocket expenses by Plaintiff and the Class in mitigation of the harm caused by Defendants include, but are not limited to, fees paid by customers who sought to cancel their cards and obtain replacement cards to protect themselves from potential unauthorized charges; fees paid by customers who had to reorder checks; fees to purchase credit reports and/or to arrange for credit monitoring and to purchase identify theft and overdraft protection; and fees paid for insufficient funds, late payment charges and overdrafts due to disrupted preauthorized charge relationships. Plaintiff and the Class suffered additional damage in that they paid for Defendants' administrative costs of data management and security, reflected as part of the purchase price of the goods charged by Defendants to Plaintiff and the Class.

CLASS ACTION ALLEGATIONS

49. Pursuant to Rules 23(a), (b)(3) and/or (b)(2) of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of himself and a nationwide class ("Class"), initially defined as follows:

> All persons or entities located in the United States who were customers of Defendants from February 22, 2009 to the present ("Class Period"), from whom Defendants collected PII that was compromised as a result of the data breaches of Defendants' card processing systems, and who sustain fraudulent charges as a result of the breach and/or made out of pocket expenditures in mitigation of the consequences to them of such data breaches. Excluded from the consumer class are governmental entities, the Defendants, any entity in which the Defendants have a controlling interest, their employees, officers, directors, legal representatives, heirs, successors and wholly or partly owned subsidiaries or affiliated companies, including parent corporations, class counsel and their employees; and the judicial officers and their immediate family members and associated court staff assigned to this case.

50. Alternatively, the Plaintiff seeks to represent two classes:

> Class 1: All persons or entities located in the United States who were customers of Defendants whose PII was compromised as a result of the data breach of Defendants' card processing systems between September and November of 2011, and who sustain fraudulent charges as a result of the breach and/or made out of pocket expenditures in mitigation of the consequences to them of such data breaches.
>
> Class 2: All persons or entities located in the United States who were customers of Defendants whose PII compromised as a result of the data

breach of Defendants' card processing systems between November and December 2012, and who sustain fraudulent charges as a result of the breach and/or made out of pocket expenditures in mitigation of the consequences to them of such data breaches.

Excluded from the classes are governmental entities, the Defendants, any entity in which the Defendants have a controlling interest, their employees, officers, directors, legal representatives, heirs, successors and wholly or partly owned subsidiaries or affiliated companies, including parent corporations, class counsel and their employees; and the judicial officers and their immediate family members and associated court staff assigned to this case.

51. The proposed Class is so numerous that individual joinder of all its members is impracticable. Due to large amount of Defendants' customers, Plaintiff believes the amount of Class members is in the hundreds of thousands. While the exact number and identities of the Class members are unknown at this time, such information can be ascertained through appropriate investigation and discovery. The disposition of the claims of the Class members in a single class action will provide substantial benefits to all parties and to the Court.

52. Pursuant to Rule 23(b)(3), there is a well-defined community of interest in the questions of law and fact involved affecting the Plaintiff and the Class and these common questions of fact and law include, but are not limited to, the following:

a. Whether the Defendants took adequate measures to protect PII;

b. Whether Defendants acted negligently in maintaining PII of hundreds of thousands of customers, even after a similar security breach;

c. Whether Defendants were negligent;

d. Whether the alleged conduct constitutes violations of the laws asserted herein;

e. Whether Defendants breached express or implied contracts with Plaintiff and the Class by failing to properly safeguard their PII and by failing to notify them of the breaches of its card processing systems and the nature and extent of their data that had been stolen as soon as practicable after such breaches where discovered;

f. Whether Defendants owed a legal duty to Plaintiff and Class members to protect their PII and whether Defendants breached this duty;

g. Whether Plaintiff and the Class members are at an increased risk of identity theft as a result of Defendants' failure to protect the Plaintiff's and the Class members' PII;

h. Whether Defendants notice to Plaintiff and Class members regarding each security breach was inadequate and unreasonably delayed; and

i. Whether Plaintiff and Class members are entitled to the relief sought, including injunctive relief.

53. Plaintiff's claims are typical of the claims of the members of the Class. Plaintiff and all members of the Class have been similarly affected by the Defendants' common course of conduct since they all relied on Defendants' representations and agreements, implied or otherwise, concerning its security of PII, and sustained damages arising out of Defendants' wrongful conduct as described herein. More specifically, Plaintiff's and Class members' claims arise from Defendants' failure to adequately safeguard Plaintiff's and Class members' PII and monitor that security, in addition to failing to notify Plaintiff and Class members timely.

54. Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel with substantial experience in handling complex class action litigation. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the Class and have the financial resources to do so.

55. Plaintiff and the members of the Class suffered and will continue to suffer harm as a result of the Defendant's unlawful and wrongful conduct. A class action is superior to other available methods for the fair and efficient adjudication of the present controversy. Individual joinder of all members of the Class is impracticable. Even if individual Class members had the resources to pursue individual litigation, it would be unduly burdensome to the courts in which the individual litigation would proceed. Individual litigation magnifies the delay and expense to all parties in the court system of resolving the controversies engendered by Defendant's course of conduct. The class action device allows a single court to provide the benefits of unitary adjudication, judicial economy, and the fair and efficient handling of all Class members' claims in a single forum. The conduct of this action as a class action conserves the resources of the parties and of the judicial system and protects the rights of the class members. Furthermore, for many, if not most, a class action is the only feasible mechanism that allows an opportunity for legal redress and justice.

56. Adjudication of individual Class members' claims with respect to the Defendants would, as a practical matter, be dispositive of the interests of other members not parties to the adjudication, and could substantially impair or impede the ability of other class members to protect their interests.

FIRST CAUSE OF ACTION

NEGLIGENCE

(On Behalf of Plaintiff and the Class, as Against All Defendants)

57. Plaintiff repeats, realleges and incorporates by reference each and every allegation contained above as if fully set forth herein.

58. Defendants owed its member customers a duty of care in the handling and safeguarding of their PII that was entrusted to them for the purpose of making purchases at Defendants' stores.

59. Additionally, Defendants assumed a duty, and had duties imposed upon them by regulations to use reasonable care to keep Class members' financial data and PII private and secure.

60. Additionally, Defendants had a duty, and had a duty imposed on them by regulations, to report the theft of PII to Plaintiff and the Class in an expedient manner (as to Data Breach One) and an immediate manner (as to Data Breach Two).

61. Defendants also represented to Plaintiff and the Class that their systems were compliant with payment card industry standards, which created a special relationship between Defendants and Plaintiff and the Class, in that Plaintiff and the Class reasonably relied on Defendants to take reasonable steps to safeguard their PII.[1]

62. In violation of their duties as set forth above and as required by law, Defendants allowed Plaintiff and Class members' information to be acquired by third parties during two breaches: Data Breach One, which occurred September 21, 2011 through November 18, 2011, and Data Breach Two, which occurred November 7, 2012 until December 5, 2012.

[1] *See* https://www.pcisecuritystandards.org/pdfs/pcissc_overview.pdf (last viewed on Jan. 11, 2013).

63. Defendant breached its aforesaid duty to use care to safeguard the PII entrusted to them by Plaintiff and the Class. Defendants' breaches include, but are not limited to, the following:

a. Failing to monitor their IT networks for the presence of foreign software in a manner that would enable them to detect this intrusion, so that he breach of security and diversion of customer information was able to continue undetected for at least two months in regard to Breach One and one month for Breach Two;

b. Failing to encrypt internal network traffic flowing between store and processor, running point-of-sales systems that were open to attack, maintaining insecure wireless connections and/or having remote access deficiencies;

c. Failing to secure its internal network credit and debit card authorization traffic from access by malware or other unauthorized parties;

d. Failing to take appropriate steps to identify and contain the security breaches when they were first discovered; and

e. Failing to appropriately limit employee access.

64. The PII of the Class that was stolen or compromised by the breach of Defendants' security includes, without limitation, information that was being improperly stored and inadequately safeguarded in violation of, among other things, industry rules and regulation.

65. The representations made to Plaintiffs and Class members created a duty of reasonable care that Defendants violated. Defendants' violations of those standards and regulations, like conforming with Payment Card Industry security

standards and providing timely notice of breaches per California Civil Code §§ 1798.82 and 1798.84(d), among others, constitute negligence per se.

66. The breach of security was a direct and proximate result of Defendants' failure to use reasonable care to implement and maintain appropriate security procedures reasonably designed to protect the nonpublic information of the Class. This breach of security and resulting unauthorized access to nonpublic information of the Class was reasonably foreseeable by Defendants, particularly, but not exclusively, due to the fact that a similar breach occurred just a year prior to Plaintiff's experience.

67. In addition, Defendants used the same company, Trustwave, to monitor security after their 2011 security breach, and to assist with the 2012 breach. Thus, there were and are no improved security measures taken. (*See* Defendants' letter from 2011 security breach, attached hereto as **Exhibit 1**).

68. Defendants were in a special fiduciary relationship with the Class by reason of their entrustment with financial data and PII. By reason of this fiduciary relationship, Defendants had a duty of care to use reasonable means to keep the nonpublic information of the Class private and secure. Defendants unlawfully breached this duty.

69. Pursuant to Class members' right to privacy, Defendants had a duty to use reasonable care to prevent unauthorized access, use or dissemination of Class members' nonpublic information of the Class private and secure. Defendants unlawfully breached this duty.

70. Defendants' failure to comply with Payment Card Industry security standards, the magnitude of the data breach, the significant delay between the date of the intrusion and the date Defendants informed the public of the breach, and previous breach in 2011 with no improved security measures, all serve as concrete evidence of Defendants' negligence and other wrongful conduct in failing to

adequately safeguard and monitor Defendants' computer systems to ensure the security of its customers' PII and financial data.

71. Defendants' violations of their duties were a substantial factor in the compromise of the Class' nonpublic information, and the resulting burden, fear, anxiety, emotional distress, loss of time spent seeking to prevent or undo any further harm, and other economic and non-economic damages to the Plaintiff and the Class.

72. As a direct and proximate result of Defendants' acts and omissions described herein, Plaintiff and the Class suffered and continues to suffer damage. Plaintiff's and the Class' damages as a result of Defendants' acts and omissions as described herein were not only the actual result of Defendants' breaches of their duties of care, but a foreseeable consequence of Defendants' failure to act with due care. Defendants' acts and omissions were also a substantial factor in the losses and damages that Plaintiff and the Class suffered and continue to suffer.

73. Defendants also had a duty to publicly disclose the data compromise in a timely manner. Timely disclosure was required so that, among other things, Plaintiff and Class members could take appropriate measures to avoid unauthorized charges on their accounts, cancel or change usernames and passwords on compromised accounts, change drivers' license numbers or state and military identification numbers and monitor their account information and credit reports for fraudulent activity.

74. Defendants breached this duty by failing to notify the public in a timely manner that information was compromised.

75. Class members were harmed by Defendants' delay because, among other things fraudulent charges have been made to Class members' accounts and Class members have wasted time and money to dispute charges with their banks.

76. Defendants knew or should have known that their computer systems for processing and storing PII and financial data had security vulnerabilities. Defendants were negligent in continuing such data processing and storage in light of those vulnerabilities and the sensitivity of the data.

77. As a direct and proximate result of Defendants' conduct, Class members suffered damages including but not limited to those set forth above.

78. Plaintiff and Class members have not in any way contributed to breach of PII and financial data in Defendants' possession or to the compromise or theft of their personal and financial data.

SECOND CAUSE OF ACTION

GROSS NEGLIGENCE

(On Behalf of Plaintiff and the Class, as Against All Defendants)

79. Plaintiff repeats, realleges and incorporates by reference each and every allegation contained above as if fully set forth herein.

80. Defendants represented that their systems were compliant with payment card industry standards.[2] However, Defendants negligently allowed Plaintiff and Class member information to be taken, in December 2012, even after a similar breach just a year before during September through November of 2011.

81. Defendants assumed a duty, and had duties imposed upon them by regulations to use reasonable care to keep Plaintiff and the Class members' financial data, and PII private and secure. By their acts and omissions described herein, Defendants unlawfully breached this duty. Plaintiff and the Class was damaged thereby.

[2] *See* https://www.pcisecuritystandards.org/pdfs/pcissc_overview.pdf (last viewed on Jan. 11, 2013).

82. The amount of care taken after the first breach by Defendants was so slight that it justifies a belief that Defendants were indifferent to the interests of the welfare of its customers (including Plaintiff and Class members).

83. The private information of Plaintiff and the Class that was stolen or compromised by the breach of Defendants' security includes, without limitation, information that was being improperly stored and inadequately safeguarded in violation of, among other things, industry rules and regulations, and consisted of PII.

84. The type of information that was given to Defendants was so sensitive in nature that as a matter of policy, a failure to exercise due care results in consequences much harsher than if the information was not of such a personal, sensitive nature.

85. Defendants did not start an investigation until it learned that customers were already experiencing credit card fraud, also inferring that security measures taken were so slight that they could not detect a security breach until customers and Class members were already harmed. And, at this point, Plaintiff and the Class' were already damaged, and subject to heightened damages because the identity theft was already well underway.

86. In addition, Defendants used the same company, Trustwave, to monitor security after their 2011 security breach, to assist with the 2012 breach. Thus, there were and are no improved security measures taken. Defendants knowingly used the same company, which results in no improved security measures and continued harm and risk of future security breaches.

87. Further, Defendants did not take adequate steps to use or strengthen their firewall and monitor data transmissions, to prevent the disclosure of PII to third parties.

88. The representations made to Plaintiff and Class members, industry standards, and regulations created a duty of reasonable care that Defendants violated. Defendants' violations of those standards and regulations, like conforming with Payment Card Industry security standards and providing timely notice of breaches per California Civil Code § 1798.82, among others, constitute negligence per se.

89. Defendants' failure to take adequate steps to protect Plaintiff and the Class' PII after Data Breach One amounted to willful, intention, or reckless conduct.

90. The breach of security was a direct and proximate result of Defendants' failure to use reasonable care to implement and maintain appropriate security procedures reasonably designed to protect the nonpublic information of Plaintiff and the Class. This breach of security and resulting unauthorized access to nonpublic information of Plaintiff and the Class was reasonably foreseeable by Defendants, particularly, but not exclusively, due to the fact that a similar breach occurred just a year prior.

91. Defendants were in a special fiduciary relationship with Plaintiff and the Class by reason of their entrustment with financial data and PII. By reason of this fiduciary relationship, Defendants had a duty of care to use reasonable means to keep the nonpublic information of Plaintiff and the Class private and secure. Defendants unlawfully breached this duty.

92. Pursuant to Plaintiff and the Class members' right to privacy, Defendants had a duty to use reasonable care to prevent unauthorized access, use or dissemination of Plaintiff and the Class members' PII and to keep their PII private and secure. Defendants unlawfully breached this duty.

93. Defendants' failure to comply with Payment Card Industry security standards (PCI DSS), the magnitude of the data breach, the significant delay

between the date of the intrusion and the date Defendants informed Plaintiff, the Class and the public of the breach, and previous breach in 2011 with no improved security measures, all serve as concrete evidence of Defendants' gross negligence and other extremely reckless or willful or intentional and wrongful conduct in failing to adequately safeguard and monitor Defendants' computer systems to ensure the security of Plaintiff and the Class' PII.

94. Defendants' violations of their duties were a substantial factor in the compromise of Plaintiff and the Class' PII, and the resulting burden, fear, anxiety, emotional distress, loss of time spent seeking to prevent or undo any further harm, and other economic and non-economic damages to Plaintiff and the Class.

95. Defendants also had a duty to publicly disclose the data compromise in a timely manner, including through notice to Plaintiff and the Class. Timely disclosure was required so that, among other things, Plaintiff and Class members could take appropriate measures to avoid unauthorized charges on their accounts, cancel or change usernames and passwords on compromised accounts, change drivers' license numbers or state and military identification numbers and monitor their account information and credit reports for fraudulent activity.

96. Defendants breached this duty by failing to notify Plaintiff, the Class and the public in a timely manner that information was compromised.

97. Plaintiff and the Class were harmed by Defendants' delay because, among other things, fraudulent charges have been made to Class members' accounts and Class members have wasted time and money to dispute charges with their banks and take other measures to safeguard their own PII after the Data Breaches.

98. Defendants knew or should have known that their computer systems for processing and storing PII and financial data had security vulnerabilities.

Defendants were negligent in continuing such data processing and storage in light of those vulnerabilities and the sensitivity of the PII data.

99. As a direct and proximate result of Defendants' conduct, Plaintiff and the Class suffered damages including but not limited to those set forth above.

100. Plaintiff and Class members have not in any way contributed to breach of PII and financial data in Defendants' possession or to the compromise or theft of their personal and financial data.

THIRD CAUSE OF ACTION

BREACH OF CONTRACT

(On Behalf of Plaintiff and the Class, as Against All Defendants)

101. Plaintiff repeats, realleges and incorporates by reference each and every allegation contained about as if fully set forth in.

102. In order to purchase restaurant food and supplies from Defendants, Defendants required that Plaintiff and the Class affirmative assent to the terms of their membership agreement and other related agreements, forming a valid and enforceable contract between Plaintiff and the Class. Further, Plaintiff and the Class were required to provide Defendants with PII, including but not limited to credit/debit card information and other personal and financial information.

103. Plaintiff and the Class believed that in giving this information to Defendants, Defendants would, in turn, safeguard that information. *See, e.g.*, privacy disclaimer of joining email list, for members only, attached hereto as **Exhibit 3**.

104. Defendants materially breached the terms of the contract(s) by its wrongful conduct alleged herein, including failing to properly secure its credit processing systems, thereby allowing Plaintiff's and the Class's sensitive PII to be compromised. Defendant further materially breached the terms of the contract(s) by failing to promptly and sufficiently notify Plaintiff and the Class that their

sensitive personal information had been compromised, depriving Plaintiff and the Class of the opportunity to mitigate their losses.

105. As a result of these breaches, Plaintiffs and the Class have been harmed as alleged herein, and have suffered and continue to suffer damage.

FOURTH CAUSE OF ACTION

BREACH OF IMPLIED CONTRACT

(On Behalf of Plaintiff and the Class, as Against All Defendants)

106. Plaintiff repeats, realleges and incorporates by reference each and every allegation contained about as if fully set forth in.

107. When providing personal and financial information and PII to Defendants in order to transact business with Defendants and utilize all services available by Defendants, Plaintiff and the Class entered into implied contracts with Defendants such that Defendants would safeguard this information and notify them promptly of any and all theft of this information.

108. Without such implied contracts, customers (including Plaintiff and the Class) would not have given their personal and financial information or PII to transact business with the Defendants.

109. Defendants breached these implied contracts they made with Plaintiff and the Class by failing to safeguard such information and failing to notify them promptly of the intrusions into their card processing systems that compromised such information.

110. The damages sustained by Plaintiff and the Class as described above were the direct and proximate result of Defendants' breaches of these implied contracts.

FIFTH CAUSE OF ACTION

VIOLATION OF CALIFORNIA'S SHINE THE LIGHT LAW (CAL. CIV. CODE § 1798.82)

(On Behalf of Plaintiff and all Class Members, as Against All Defendants)

111. Plaintiff repeats, realleges and incorporates by reference each and every allegation contained above as if fully set forth herein.

112. On information and belief, Plaintiff believe that his and other Class members' PII, credit/debit card information and other personal and financial information had been compromised from about mid-September 2011 through mid-November 2011. Defendants did not notify customers, including Class members until at least November 25, 2011. Defendants became aware of the breach on November 9, 2011.

113. Data Breach One was approximately two months long but customers were not notified until over two months after the breach began, and nearly three weeks since Defendants' discovery of the security breach. This was an unreasonable delay in violation of California Civil Code § 1798.82, because all the facts Defendants needed to know were available to Defendants immediately - that customer data had been accessed by at least one unauthorized third party.

114. The delayed notification after Data Breach One was not made in the most expedient time possible, as required by California Civil Code § 1798.82.

115. On December 4, 2012, Defendants learned that Class members' PII, credit/debit card information and other personal and financial information had been compromised in the course of Data Breach Two. Upon further investigations, Defendants learned that this breach occurred starting on November 7, 2012. Defendants did not notify Plaintiff or Class members for at least another two weeks, in violation of California Civil Code §§ 1798.82 and 1798.84.

116. This was an unreasonable delay because all the facts needed to know were available to Defendants on December 4, 2012 - that customer information had

been compromised customers were already experiencing credit card fraud. This delayed notification of 2012 was not made in the most expedient time possible, as required by California Civil Code §§ 1798.82 and 1798.84.

117. Pursuant to California Civil Code § 1798.82(j) Plaintiff seeks an order requiring Defendants to make prompt and detailed disclosure to Plaintiff and Class members of the type of information that was compromised and requiring Defendants to notify Plaintiff and Class members of any future security breaches immediately and with sufficient detail. Plaintiff and the Class also claim damages, statutory damages, attorney's fees and costs under Civil Code § 1798.84.

SIXTH CAUSE OF ACTION
VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW
(CAL. BUS. & PROF. CODE §§ 17200, *et seq.*)
(On Behalf of Plaintiff and all Class Members, as Against All Defendants)

118. Plaintiff repeats, realleges and incorporates by reference each and every allegation contained above as if fully set forth herein.

119. California's Unfair Competition Law, Business and Professions Code § 17200 (the "UCL") prohibits any "unfair competition," including any "unlawful, unfair or fraudulent business act or practice" and "unfair, deceptive, untrue or misleading advertising." For the reasons discussed above, Defendants engaged in unlawful, unfair, and/or fraudulent business practices in violation of the UCL.

120. Defendants' conduct was unlawful through violation of the Shine the Light Law, set forth above, and through Defendants' negligence, gross negligence, breach of express contract, breach of implied contract, and violations of consumer fraud statutes and data security and privacy statutes of this state and other states in the United States. Plaintiff and the Class reserve the right to allege at trial other violations of law which constitute other unlawful business acts or practices.

121. Defendants' acts and omissions described herein were also unfair in that they were contrary to the public policy of California and other states with laws

similar to the Shine the Light law. For example, the Shine the Light Act states: "It is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own or license personal information about Californians to provide reasonable security for that information." Cal. Civ. Code § 1798.81.5.

122. Defendants' acts and omissions as described herein were also fraudulent in that Defendants represented to Plaintiff and the Class that they used adequate and industry standard data security management and protection protocols, equipment and procedures, when that representation was either false, failed to disclose complete information so as to make it truthful, or Defendants remained silent about facts when they had a duty to disclose them to Plaintiff and the Class.

123. Defendants' further misrepresented the steps they were taking and would take to remedy the theft, loss, or disclosure of PII after Data Breach One, and Plaintiff and the Class reasonably relied on Defendants' representations that Defendants' Data Breach One problems had been remedied, when such representation was either false, failed to disclose complete information, or Defendants remained silent about facts that they had a duty to disclose, all of which information Plaintiff and the Class would have considered material in keeping their PII on file with Defendants, whether as a member or for the purpose of making a future purchase from Defendants.

124. As a result of Defendants' unfair competition, Plaintiff and the Class have suffered injuries in fact and have lost money, as described herein.

125. Defendants have thus engaged in unlawful, unfair and fraudulent business acts and practices, entitling Plaintiff to injunctive relief against Defendant, as set forth in the Prayer for Relief.

126. Defendants were also unjustly enriched by their acts and omissions as described herein because Plaintiff and the Class paid for Defendants'

administrative costs of data management and security, reflected in the increased purchase price of Defendants' goods, versus companies that sell similar goods but maintain adequate data security and management protocol, equipment and procedures. Had Defendants engaged in fair business conduct, Plaintiff and the Class could have taken their business elsewhere both before and after Data Breach One, which conduct by Defendants harmed not just Plaintiff and the Class as detailed herein, but the public.

127. Defendants accordingly owe Plaintiff and the Class restitution and disgorgement for the data breaches that may have been acquired by Defendants' unlawful, unfair or fraudulent business conduct.

128. Pursuant to Business and Professions Code § 17203, Plaintiff seeks an order requiring Defendants to immediately cease such acts of unlawful, unfair and fraudulent business practices.

PRAYER FOR RELIEF

129. Wherefore, Plaintiff, on behalf of himself, all others similarly situated and the general public, pray for judgment against the Defendants as to each and every cause of action, including:

A. An order declaring this action to be a proper Class Action and requiring Defendants to bear the costs of Class notice;

B. An order awarding declaratory and injunctive relief as permitted by law or equity, including enjoining Defendants from continuing the unlawful practices as set forth herein;

C. An order awarding damages to Plaintiff and the Class in an amount to be determined at trial;

D. An order awarding Plaintiff and the Class their reasonable litigation expenses and attorneys' fees;

E. An order awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable;

F. An order awarding restitution and disgorgement of Defendant's revenues from the breaches of implied contracts to Plaintiff and the proposed Class members;

G. Punitive damages for Defendants' willful, reckless, or intentional conduct;

H. Statutory damages under California Civil Code § 1798.84;

I. An order compelling Defendant to engage in a more secure method of storing and protecting customer information;

IJ. An order providing for all other such equitable relief as may be just and proper.

JURY DEMAND

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: February 22, 2013

/s/ Ronald A. Marron

By: Ronald A. Marron

LAW OFFICES OF RONALD A. MARRON, APLC
RONALD A. MARRON
SKYE RESENDES
3636 4th Avenue, Suite 202
San Diego, California 92103
Telephone: (619) 696-9006
Facsimile: (619) 564-6665

Attorneys for Plaintiff and the Proposed Class